

# Structural Causes and Cyber Effects

## Why International Order is Inevitable in Cyberspace

*James Wood Forsyth Jr.*  
*Maj Billy E. Pope, USAF*

*That is the essence of science: ask an impertinent question, and you are on the way to a pertinent answer.*

—Jacob Bronowski

### Abstract

As the distribution of power in the world changes, the structure of international politics will change from unipolarity to multipolarity. This will usher in a period of intense oligopolistic competition, particularly in cyberspace, where the actions of one great power will have a noticeable effect on all the rest. To soften the harsh effects of multipolarity and oligopolistic competition upon cyberspace, the great powers will have no good choice but to cooperate and create rules, norms, and standards of behavior to buttress what will essentially be a new political order—one where its “members willingly participate and agree with the overall orientation of the system.”<sup>1</sup> Since cyberspace is part and parcel of that system, order within it is inevitable. Unhinging the mysteries of cyberspace is merely contingent upon analysts’ abilities to conceptualize the domain in the language of international politics. Should they choose to do so, they might come to realize that the extraordinary problem of cyberspace is but an ordinary one in the life of states.



Will international order—the kind that is essential to sustain the elementary goals of the society of states—emerge in cyberspace? Our

---

Dr. James Wood Forsyth Jr. currently serves as professor of national security studies, USAF School of Advanced Air and Space Studies (SAASS), Maxwell AFB, Alabama. He earned his PhD at the Josef Korbel School of International Studies, University of Denver. He has written on great-power war, intervention, and nuclear issues.

Maj Billy Pope, USAF, is a cyber operations officer and commander of the 81st Communications Squadron. He holds an MPA degree from Harvard’s Kennedy School of Government, a Master of Military Strategy from SAASS, and is a PhD candidate studying the ethics of cyber warfare.

Report Documentation Page			Form Approved OMB No. 0704-0188		
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE <b>2014</b>	2. REPORT TYPE		3. DATES COVERED <b>00-00-2014 to 00-00-2014</b>		
4. TITLE AND SUBTITLE <b>Structural Causes and Cyber Effects: Why International Order is Inevitable in Cyberspace</b>			5a. CONTRACT NUMBER		
			5b. GRANT NUMBER		
			5c. PROGRAM ELEMENT NUMBER		
6. AUTHOR(S)			5d. PROJECT NUMBER		
			5e. TASK NUMBER		
			5f. WORK UNIT NUMBER		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) <b>Air Force Research Institute (AFRI), Strategic Studies Quarterly (SSQ), 155 N. Twining Street, Maxwell AFB, AL, 36112</b>			8. PERFORMING ORGANIZATION REPORT NUMBER		
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSOR/MONITOR'S ACRONYM(S)		
			11. SPONSOR/MONITOR'S REPORT NUMBER(S)		
12. DISTRIBUTION/AVAILABILITY STATEMENT <b>Approved for public release; distribution unlimited</b>					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT <b>As the distribution of power in the world changes, the structure of international politics will change from unipolarity to multipolarity. This will usher in a period of intense oligopolistic competition, particularly in cyberspace, where the actions of one great power will have a noticeable effect on all the rest. To soften the harsh effects of multipolarity and oligopolistic competition upon cyberspace, the great powers will have no good choice but to cooperate and create rules, norms, and standards of behavior to buttress what will essentially be a new political order??? one where its ???members willingly participate and agree with the overall orientation of the system.???1 Since cyberspace is part and parcel of that system, order within it is inevitable. Unhinging the mysteries of cyberspace is merely contingent upon analysts??? abilities to conceptualize the domain in the language of international politics. Should they choose to do so, they might come to realize that the extraordinary problem of cyberspace is but an ordinary one in the life of states.</b>					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT <b>Same as Report (SAR)</b>	18. NUMBER OF PAGES <b>18</b>	19a. NAME OF RESPONSIBLE PERSON
a. REPORT <b>unclassified</b>	b. ABSTRACT <b>unclassified</b>	c. THIS PAGE <b>unclassified</b>			

answer is “yes.” International order in cyberspace is contingent upon structural change; achieving it has more to do with power and competition than it does with concerns over sovereignty, freedom of speech, or democracy. And since power and competition are constantly being negotiated in international life, international order within cyberspace is unavoidable. Because this is an unconventional claim, it is important to elaborate the argument.

The distribution of power in the world is changing. As it does, the structure of international politics will change from unipolarity to multipolarity. This will usher in a period of intense oligopolistic competition where the actions of one great power will have a noticeable effect on all the rest. To soften the harsh effects of multipolarity and oligopolistic competition, the great powers will have no good choice but to cooperate and create rules, norms, and standards of behavior that shore up what will essentially be a new political order—one where its “members willingly participate and agree with the overall orientation of the system.”<sup>2</sup> Since cyberspace is part and parcel of that system, order within it is inevitable.

The argument proceeds as follows: We begin by reviewing the role power plays in international politics. Next, we examine the “extraordinary” nature of cyberspace and then detail the causal relationship between the distribution of power and cyber effects. Lastly, we offer a preview of the forthcoming cyber regime.

## **What Every Realist Knows**

Order within cyberspace, like order within the sea, air, and space, is contingent upon international structure. Structure—be it uni-, bi-, or multipolar—is the result of the uneven distribution of power throughout the world. Yet, *power* is a vexing word. While it might be hard to define, it is not hard to recognize. In its simplest sense, power refers to a state’s economic and military capabilities. These capabilities provide the means to achieve autonomy, permit a wide range of actions, increase margins of safety, and, in the case of the great powers, provide its possessors a greater stake in the management of the system.<sup>3</sup> Thus power—unevenly divided—plays an important role in international politics; it sets up a world of strong and weak states, highlighting the roles played by the great powers.

What is a great power? As Martin Wight put it, great powers are states with “general interests, whose interests are as wide as the states-system itself, which today means worldwide.”<sup>4</sup> Hedley Bull clarified this further by claiming that great powers were members of a club who were comparable in status, in the front rank of military power, and were recognized by their own leaders and peoples to have “special rights and duties.”<sup>5</sup> From this last criterion, great power is a role.

To think of great power as a role is to think in terms of international order. *International order* refers to a “pattern of activity that sustains the elementary or primary goals of the society of states.”<sup>6</sup> This includes the preservation of the society of states and maintaining the independence of states, peace, and those goals essential for the sustainment of international life such as the limitation of violence, keeping of promises, and possession of property.<sup>7</sup>

To think in terms of international order is not to suggest that international politics are orderly.<sup>8</sup> They are not. International politics are anarchic. *Anarchy* does not mean chaos, however. It refers to the absence of rule or a hierarchical order based on formal subordination and authority. There is considerable order in an anarchic international system, but that order is not hierarchic like the one found in domestic politics. As Bull saw it, great powers contributed to international order in two ways: they managed relations among themselves, and they exploited their preponderance of power in such a way as to “impart a degree of central direction to the affairs of international society as a whole.”<sup>9</sup> They do this by creating political orders that are “legitimate and durable.”<sup>10</sup>

Legitimate political orders are ones in which “members willingly participate and agree with the overall orientation of the system.”<sup>11</sup> Once in place, these orders tend to facilitate “the further growth of inter-governmental institutions and commitments.”<sup>12</sup> Such arrangements create deeper institutional linkages among states and make it difficult for alternative orders to replace existing ones. Thus, legitimate political orders are transformative ones, making their dissolution difficult if not impossible. Moreover, there is a functional imperative for strong states to cooperate and seek institutional solutions—they allow for the conservation of power itself. In essence, strong states must make their “commanding power position more predictable and restrained,” which makes the creation of rules a necessity.<sup>13</sup>

Rules represent the fundamental normative principle of international politics, which today refers to the society of states. There is nothing sacrosanct about the society of states, but few would deny that it represents the fundamental principle of political organization (as opposed to a universal empire or a cosmopolitan community of individual human beings). Thus, rules are essential for international life; they are devised by the great powers to provide guidance for what is and what is not acceptable behavior.<sup>14</sup>

If great powers cooperate to create rules to shore up international order, why haven't they done so in cyberspace? Part of the answer has to do with normative differences. That is to say, concerns over sovereignty, freedom of speech, and democracy have kept the great powers from devising a set of principles to fully govern cyberspace. But the root cause of this disagreement is structural. While great powers can do more than most, no state—no matter how strong—can do all it wants, all the time. A good example is the United States today.

Not only is the United States expected to ensure that order exists within the world, but it is also expected to ensure that an equitable distribution of public goods exists throughout the world. Couple this with the demands of fighting two long wars and one gets the idea: There are limits to what states can do in this world. This raises a profound theoretical question: Is unipolarity an ideal condition for creating order in cyberspace, or in any other domain for that matter?<sup>15</sup> Historically, such large responsibilities have been shared among several great powers. Importantly, however, therein lies the rub: international structures do not last forever; they change, and when they do, order changes with them.

Yet, cyber authors appear reluctant to embrace the structure-order relationship. This might be due to the fact that the domain has yet to be adequately conceptualized within the thicker pattern of international politics. As it stands today, cyberspace appears to exist all by itself—affected by nothing, restrained by no one.<sup>16</sup> But is this the case? Does cyberspace stand alone? Hardly. Cyberspace is a man-made domain or realm of activity, and therefore, order within it depends upon international order, writ large. Because of this, governments—*states*—are not out of the picture; they are as prevalent as ever. As states become more dependent on cyberspace, those who can afford to devise and maintain the physical infrastructure—high-speed, undersea fiber-optic cables and satellite downlinks—and those that have migrated more of their func-

tions to cyberspace will enjoy a competitive advantage over all others. Those same states will want to protect their large capital investments, making the creation of rules, norms, and standards of behavior a political necessity. But one searches in vain to find a theorist who conceptualizes the domain in such ordinary terms. Everything about cyberspace appears to be “extraordinary.” To highlight this last point, a brief review is in order.

## **The Extraordinary Nature of Cyberspace**

Cyberspace is extraordinary. At least that is a central theme of some of the popular literature surrounding the topic. And indeed, the domain has some exceptional qualities—it is ubiquitous and barriers to entry are low. In the language of international politics, it is a common property resource in that no one can be excluded from it. Yet, in their descriptions of the domain, some writers tend to misconstrue the very thing they are attempting to describe. One quotation can serve for many others. Cyberspace is “a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.”<sup>17</sup> Note the author’s emphasis upon interdependence. In international politics, interdependence means dependence—two or more parties are thought to be interdependent if they depend on one another equally for the supply of goods and services.<sup>18</sup> Yet “interdependence” has been used by analysts to explain nearly every major occurrence in international life, to include the causes of war (as in the case of World War I) and the prevention of war (as in the case of today’s economic interdependence). The common misuse of the term *interdependence* begs the question: Just what, precisely, is cyberspace dependent upon? Here the Internet, networks, systems, and processors appear to float freely. Collectively, they might be dependent upon one another, but their relationship with the “global domain” and “information environment” is difficult to decipher. They might be dependent upon the “grid” or World Wide Web, but they might be dependent upon nothing, and nothings cannot be interdependent.

It is not much different in some of the scholarly literature, where again one quotation can serve for others. “Cyberspace is growing rapidly and transforming, if not yet superseding, the manner in which we

conduct ourselves in business, politics, and entertainment. . . . The challenge for practitioners, strategic planners and policymakers is to understand the nature and extent of these changes.”<sup>19</sup> Note the emphasis on “change.” Not only does change move in one direction, but its movement easily traverses several realms of social activity—business, politics, and entertainment—as if it were shot out of a cannon, unencumbered by any sort of structural restraint. Now suppose that cyberspace is the cause of such change. How would one go about proving it scientifically? Step one would be to state the theory to be tested. Step two would devise hypotheses to be tested. But since no general theory of cyberspace exists, no hypotheses can be inferred. The best one can conclude is that cyberspace might be changing things, but for now at least it is hard to ascertain how.

It is even worse when it comes to war, something that many cyber authors claim to know something about. Take this assertion, for example: “Cyber war is real; it happens at the speed of light; it is global; it skips the battlefield; and, it has already begun.”<sup>20</sup> Or this: “Potentially the biggest change to the existing character of warfare, and therefore the most substantial challenge to the nature of war, is provided by Strategic Information Warfare.”<sup>21</sup> And finally, there is this: “network-centric warfare may yet come to be retrospectively viewed as merely the birth pangs of a truly future *chaoplexic* regime in the scientific way of warfare.”<sup>22</sup> We had better pause to ask: what is all this for? In the first instance, cyber war is devoid of any empirical qualities. In the second and third instances, the old language of war no longer applies. Apparently, the great change that is upon us—cyberspace—has given way to a new form of war that no one can see, measure, or presumably fear. Not all of these influential authors are equally dire, but when thinking and writing about cyberspace, extraordinary is the order of the day.

How can one explain this? One word: *exuberance*. Every version of cyberspace noted above expresses the “feeling of being swept into the future by irresistible forces.”<sup>23</sup> Given the novelty of the domain, this is understandable. And while there is nothing inherently wrong with stressing the uncommon nature of things, extraordinary claims are not without consequence. They can obscure what is ordinary about the phenomena in question. Put simply, by stressing the extraordinary nature of cyberspace, analysts have failed to make the rather ordinary connection between political structure and order. For one reason or another,

cyber authors have overlooked how changes in the distribution of power throughout the world will relate to changes in cyberspace. While it is true that cyberspace is changing things (and perhaps even superseding things), the structure of international politics is changing, too. And as it does, cyberspace will inevitably change with it.

## **Structural Causes**

How will a change in structure result in changes to order? The answer has to do with the distribution of power throughout the world. To illustrate, a brief review is necessary. In 1700, seven great powers shared the bulk of the world's material capabilities; in 1800, just five. By 1910, that number had grown to eight; yet by 1935, it had slipped to seven. Following World War II, only two great powers remained: the Soviet Union and the United States.<sup>24</sup> What does this suggest?

Multipolar structures are the historical norm. In the past 300 years, there has been only one period of bipolarity followed by a single period of unipolarity. Second, historic global change can come quickly and without much warning. In 1910, eight great powers held significant portions of the world's material capabilities; in 1945, just two. Third, structural change is a regular occurrence in international life, which is why it is important to begin any analysis of cyberspace from the perspective of the distribution of power. The distribution of power throughout the world is changing.

Brazil, Russia, India, and China are poised to become the four most dominant economies by the year 2050. And while it has become cliché to suggest that these states will inevitably rival the United States, it is important to stress that these four states encompass more than 25 percent of the world's land coverage and 40 percent of the population, while holding a combined GDP of approximately \$12.5 trillion. Three are nuclear powers that collectively comprise the world's largest nuclear entity, spending nearly \$336 billion on defense. Hardly an alliance, they have taken steps to increase their political cooperation, mainly as a way of influencing the US position on trade accords.

What does the current redistribution of power mean for the world? All things being equal, it means that the structure of international politics will revert to its historical norm, multipolarity, which will usher in an intense period of oligopolistic competition. This structural change



will, in turn, create incentives for the great powers to cooperate when considering matters of grave importance like cyberspace, even if they would prefer not to. Two points illustrate why.

In unipolar worlds, like we have been living in for the past 25 years, the strongest state holds a monopoly of power, and the system is pliable, at least for that state. Since the system is pliable, policymakers' fears of competition are reduced, so they tend to be emboldened and prone to risk and overextension. The recent wars in Afghanistan and Iraq are illustrative. Since no state (or combination of states) was capable of preventing the United States from going to war, US policymakers readily accepted risk and consistently undervalued the costs of war.

But in multipolar worlds, where power is shared among several states, policymakers have to act with deliberate restraint, carefully plotting their courses of action in terms of how others in the group will react, even if they might prefer not to. Like firms in a competitive market, states in oligopolistic competition want as few in the group as possible. Each watches the other closely for fear of being driven out of the market. Thus, members of an oligopolistic group must be sensitive to each other's actions, while considering the reactions that they might provoke. With respect to incentives, where unipolarity liberates, multipolarity constrains.<sup>25</sup>

Learning how to live in world of constraints will not be easy for US policymakers, but it will be necessary. One can expect challengers to compete with the United States in every domain or realm of activity. In economic terms, this could stoke fears of cutthroat competition. In military terms, the diffusion of technology might enable challengers to rapidly pursue technologies that counter US ones. But does the emergence of rivals necessitate a return to the "war of all against all?" Some might think so—we know the logic: competition leads to conflict; conflict leads to war. But there is every reason to think that as the distribution of power throughout the world changes, cooperation among the great powers will increase.<sup>26</sup> Why?

As the world transitions from unipolarity to multipolarity—as the structure of international politics changes—the collective dependencies upon the sea, air, space, *and* cyber will intensify. As dependencies intensify, the constraining effects produced by multipolarity and oligopolistic competition will be readily felt by all. Unlike today, where one great power—the United States—can do mostly what it wants, most of the time, the actions of one great power will have a noticeable effect on all

the rest. In such a world, the fortunes and security of each will be tightly coupled to the fortunes and security of the others, and as a result, the great powers will be incentivized to cooperate. Nothing will be more important to the great powers than creating and maintaining international stability and order whereby they, and all others, can thrive. To meet these demands, the great powers will cooperate and create rules, norms, and standards of behavior that shore up the new political system. Cyberspace will remain a critical part of that system and order within it is inevitable.

## **Cyber Effects**

No one can predict when the structure of international politics will change—international politics does not work with Newtonian fidelity. As to the effects those changes will have on cyberspace, two points are worth stressing. First, international order within cyberspace will not mean harmony; states will quarrel with, cheat, and attempt to defect from the forthcoming cyber regime. Second, there is no telling what the normative makeup of a cyber order might be. Will it promote democracy? Or will it result in the creation of a digital “Iron Curtain” with governments attempting to limit who can do what, when, where, and how in cyberspace? Again, one cannot be certain. But as power continues to be redistributed throughout the world, the effects of cyberspace are making themselves known. In this section, we examine those effects and assess their likely impact on international politics.

First, there is no question that cyberspace is affecting domestic politics. The virtual realm—specifically Facebook, Twitter, and SMS text messaging—was a force behind the 2011 social revolution in Egypt that drove Hosni Mubarak from power after 30 years of dictatorial rule.<sup>27</sup> Domestic leaders facing similar circumstances around the world took notice. Turkey instituted bans on several forms of social media during its own civil unrest in 2014.<sup>28</sup> Generally, citizens who are physically excluded from presenting dissenting views can find respite atop the relatively anonymous platforms cyberspace provides. From their electronic sanctuary, domestic groups find ways to vent frustrations, reinforce shared beliefs, recruit new members, and create plans.

But the effects of cyberspace are not limited to domestic strife. For state and nonstate actors, cyberspace is a fringe environment where accepted

norms of behavior lag just enough to permit acts that would be deemed unacceptable in other areas. The Syrian Electronic Army (SEA), for example, is a loosely affiliated group of programmers and activists within Syria that aims to counter potential US involvement in Syria's ongoing civil struggle. The SEA launched a wave of cyber attacks against US interests in 2013–14 while hidden in the ambiguity of cyberspace. These attacks defaced numerous US information systems and even brought down the *New York Times* website for an entire day. Physical attacks that produced the same level of disruption would have left attackers exposed to potential retaliation or physical harm. In general, cyberspace allows electronic combatants unprecedented freedom to maneuver.

Secondly, as cyberspace becomes entrenched in the day-to-day affairs of governance, one can assume that diplomatic relations will contain both traditional and cyber threads. Take diplomatic relations between South Korea, the United States, and North Korea. In June 2013, as tensions ran high between Kim Jong-Un's regime and the international community, the hacker group, Anonymous, made a splash with claims that they had infiltrated North Korean computer networks.<sup>29</sup> While many of Anonymous' claims were later refuted, the timing of their announcement might have obfuscated diplomatic relations and escalated that conflict.

While cyberspace is making its effects known both domestically and diplomatically, the most significant effects are found in the realm of economics. Commercial entities are producing effects that states must heed. Obviously, companies like Google, Microsoft, and Facebook play an important role in the functionality of cyberspace. By providing the computing environments, data, and directory systems on which the Internet and its larger social connections rely, these companies and others like them have made themselves economically indispensable. States that wish to remain competitive in the global marketplace must, in some respects, acquiesce to their demands. In this regard, globalized markets for goods and services have usurped traditional domestic-only economies.<sup>30</sup> These efficient, interconnected networks are completely reliant on a constant flow of information to facilitate complex supply and production arrangements.<sup>31</sup> For developed and developing economies, the message is simple: living "off the grid" is becoming untenable.

Just as cyberspace is producing instantaneous information flows in the global political economy, international order is being influenced by

the immediate access to information. Governments, citizens, and corporations have greater access to information—or global situational awareness—than at any time in history, and with greater information comes competitive advantage. Not only are actors better informed, they are more sensitive to advantages and disadvantages, potential threats, and perceived legitimacy. They are also keenly aware of the newly demarcated playing field. Those states on the grid enjoy economic benefits others do not.

Yet, as potent as these capabilities might be, the effects that cyberspace produces in no way usurps the fundamental normative principle of international politics, which remains the society of states. Even in the most extreme cases—that of the Arab Spring in Tunisia and Egypt—social media only went as far as to help dethrone existing power structures. Governments emerging in the aftermath of these revolutionary events are doing so in the ordinary sense—with citizens using traditional forms of power and influence to decide “who will lead.” No doubt, cyberspace is playing a role in the evolution of international politics, but virtual relationships—political or social—remain subservient to the exigencies of the great powers. So long as the society of states exists, which is to say so long as people rely on the state for security and well-being, the great powers will inevitably leverage cyberspace to enhance rather than undermine its existence. This in no way trivializes the importance of cyberspace. Today, every state faces a cyber-security dilemma—living both on and off the grid creates vulnerabilities that complicate daily life. For no other reason than survival, states will have no choice but to work together to modulate these vulnerabilities.

## **The Future Cyber Regime**

Cyberspace poses challenges, but challenges are nothing new in international politics. In fact, the short history of the international system is one of adaptation and resiliency. Here, regimes have played a useful role. They assist the great powers in coordinating, provisioning, and distributing public goods. Regimes are defined as “principles, norms, rules, and decision-making procedures around which actor expectations converge in a given issue-area.”<sup>32</sup> They can be found in nearly every corner of international political activity, to include trade (in the form of the World Trade Organization), security (with the Non-Proliferation Treaty) and

human rights (with the UN Declaration of Human Rights).<sup>33</sup> Thus, as we sketch out the coming cyber regime, it is useful to recall how other security regimes developed. The arms control regime is illustrative.

In the past, the idea of nuclear deterrence was a concept that “could neither be taken for granted nor ruled out.”<sup>34</sup> Over time, as scientists and strategists became aware of the lethality of nuclear weapons and concerned about the fear of surprise attack, a consensus emerged around the idea that security could be enhanced through arms control.<sup>35</sup> As the group matured, it reached into the highest offices of government and turned ideas into policies that impacted both the United States and the Soviet Union. The initial regime—comprised of concerned scientists and strategists—was “a necessary precondition” for the forging of the superpower-led arms control regime that followed.<sup>36</sup> That regime—essentially a great-power condominium—created a set of rules and norms that exercised considerable influence on international security policy. Its most significant achievements—including the ABM Treaty, SALT I and II, START I–III, SORT, and New START—made conflict resolution in the form of arms control an option preferable to nuclear war, even between two antagonistic, heavily armed rivals. Like nothing before it, the arms control regime created rules, norms, and standards of behavior that brought order to what was highly contested and valuable terrain.

While the analogy between cyberspace and arms control can be taken too far, comparing the two fields from a policy perspective is useful. The concept of mutual vulnerability set the conditions necessary for the nuclear powers to create the rules and treaties noted above. Similar vulnerabilities exist in cyberspace today. Maj Gen Brent Williams, the USCYBERCOM director of operations, noted in his article “Ten Propositions Regarding Cyberspace Operations” that “in cyber, the offender enjoys some inherent advantages over the defender.”<sup>37</sup> In the absence of technical protective measures that are able to thwart attacks, then rules, norms, and standards of behavior become the *de facto* methods by which states check one another. As nations become more dependent upon cyberspace for basic security functions, these will take on even greater importance.

For comparative purposes, it is important to stress that the rules and norms governing arms control did not spring into existence overnight. They evolved as global power became more divided among the superpowers and as ideas and practices orbited within the minds and habits

of concerned scientists and practitioners.<sup>38</sup> Judging from the volume of literature on the subject, one can deduce that a similar community of scholars and policymakers exists that shares a common concern about cyberspace—even if members cannot agree on what to do about it. Might this be a precondition for the emergence of a cyber regime? We believe it is. Therefore, with the arms control regime in mind, it is not difficult to visualize how a cyber regime would “impart a degree of central direction to the affairs of international society as a whole.” A cyber regime could assist in this by creating rules and norms that strengthen legal liability, reduce transaction costs, and mitigate uncertainty.

Reflecting upon the growth of legal liability in cyberspace, Gary Brown and Keira Poellett conclude, “In the absence of formal international agreements, cyber custom is beginning to develop through the practice of states.” Yet, while there has been “some movement toward declarations, agreements, treaties and international norms in the area, the hopeful statements most often heard do not coincide with current state practice.”<sup>39</sup> It is worth noting that similar concerns existed before the advent of the International Telecommunication Union (ITU). Today, the ITU is an intergovernmental organization with broad authorities in the area of global communications governance.

Yet, all is not well with the ITU. Sharp disagreements exist regarding its authorities and responsibilities. To get a handle on the current state of play, it is useful to recall how the Internet and cyberspace evolved. A small network of computers produced through a joint government, commercial, and academic venture grew into the massive interconnected structure of today. The systems that run the Internet—namely the Domain Name System (DNS) that provides addressing and presence for devices in cyberspace and the vast fiber optic, satellite, and airwave infrastructures that facilitate connections—grew out of a foundation built on openness and collaboration. The US government, while not in a position of direct control, certainly played an influential role in the early Internet environment. Today, however, the vast majority of the Internet’s backbone, services, and software platforms are managed by the commercial sector. The cyberspace community is made up of the world’s citizenry. Government plays a lesser role. This is evidenced by the US decision to relinquish what little control it retained over the Internet’s DNS to an international consortium of stakeholders in 2015 “to support and en-

hance the cooperative multistakeholder model of Internet policymaking and governance.”<sup>40</sup>

Not all states are keen to accept such a cooperative approach. A chasm has developed among countries like Russia and China who want to play a more active role in determining the shape and content of their internet spaces and those like the United States and Britain who do not. At stake is the future of Internet governance, which is a significant concern but a subset of cyberspace in general. Listening to the debates, it appears as if the Internet is about to implode along national lines, with countries choosing directions all their own. But is this realistic? Perhaps, but even when states disagree, compromise is possible, as the making of arms control agreements illustrates. Thus we would suggest that this “debate” is a bit of a red herring; even liberal democracies comprehensively manage their Internet spaces. While most regulation is discreet—or safely hidden within the intelligence services—liberal democracies are constantly on the lookout for spies and cyber criminals. So it is not as simple as free and open versus not free and closed. That said, should the “cyber-sovereignists” have their way, they might unravel the idea of multistakeholder Internet governance entirely—so the stakes are high.

Given this, a window of opportunity exists for the liberal democracies to go on the offensive. One strategy gaining some momentum is to turn the Internet into a human rights issue. This would instantly upgrade the status of the Human Rights Committee, but the outcome is uncertain. On the one hand, it could galvanize the democracies. On the other, it could do the same for the opposition, widening the chasm. Another strategy might be to “cut bait” and allow states to go it alone. This would free the United States and other like-minded states to forge ahead with an open Internet, while others restrict their own. Creating an altogether separate cyberspace environment without connections to the Internet’s existing hierarchy of management and addressing systems would be an extraordinarily expensive technical undertaking. More likely, countries will attempt to shape their portions of the Internet through creative firewall and filter systems, as China, Russia, and many Middle Eastern countries have done. *But if these countries choose to remain dependent upon the core management systems of the global cyberspace environment, they will have no choice but to reluctantly cooperate with the rules, norms, and standards of behavior embodied in the emergent cyber regime.*

International regimes also affect transaction costs, and not just in the mundane way of being cheaper. Currently, there is a network of organizations that provides forums and secretaries who work to establish rules and principles governing the Internet. And even though it might seem like the Internet is up for grabs, these organizations are functionally differentiated, making the practice of Internet governance a division of labor. We have mentioned the ITU, but the Internet Corporation for Assigned Names and Numbers (ICANN) currently supervises the DNS, manages top-level Internet domains, and oversees root servers that provide access to information on the Internet. The Internet Society develops standards for operating the Internet and its overall architecture, while the World Wide Web Consortium (W3C) develops standards for the Web.


Lastly, regimes reduce uncertainty. They do this by creating expectations of reliability, common knowledge within a community about a particular issue, and by reinforcing cooperation itself. With respect to the world trade regime, the G8 summit is a good example. The annual G8 meeting has created expectations of reliability and a sense of conformity as to what is and what is not acceptable behavior. It rests on common knowledge—or shared information that reduces risk. Moreover, each summit reinforces the practice of international summitry itself. It can also punish defectors, as is the case with Russia today.

As sketched out here, a cyber regime will not “solve” all of the challenges posed by cyberspace. States will continue to quarrel with, cheat, and defect from the cyber regime. Nonstate actors, too, will continue to pose grave challenges to international order within cyberspace. But by strengthening legal liability and reducing transaction costs and uncertainty, a cyber regime will assist states as they come to terms with these challenges.

## **Conclusions**

There is room for optimism when thinking about cyberspace, but that optimism does not stem from the “better angels of our nature.” It stems from the ordinary nature of power and competition. Cyberspace will inevitably be what the great powers make it. Unhinging its mysteries is not alchemy or a pipe dream; it is merely contingent upon analysts’ abilities to conceptualize the domain in the language of international politics. Should they choose to do so, they might come to



realize that the extraordinary problem of cyberspace is but an ordinary one in the life of states. 

## Notes

1. G. John Ikenberry, *After Victory: Institutions, Strategic Restraint, and the Rebuilding of Order after Major Wars* (Princeton, NJ: Princeton University Press, 2001), 52.
2. Ibid.
3. Kenneth Waltz's structural realism demarcated the field of international politics into two groups: those close to or those far away from his ideas. We use those ideas throughout to explain why order within cyberspace is inevitable. See Waltz, *Theory of International Politics* (New York: McGraw-Hill, 1979).
4. Martin Wight, *Power Politics* (New York: Continuum, 1978), 50.
5. Hedley Bull, *The Anarchical Society: A Study of Order in World Politics* (New York: Columbia University Press, 1977), 196.
6. Ibid., 8.
7. Ibid., 16–19.
8. Presumably, a disordered state of international affairs would exist if a pattern of activity did not exist that sought to preserve the society of states, the independence of states, and the preservation of peace and associated goals such as the limitation of violence. One might infer that this is the case today within some states. However, while the internal makeup of some states might be fractured, the integrity of the international society of states today is not.
9. Bull, *Anarchical Society*, 200.
10. Ikenberry, *After Victory*, 52.
11. Ibid.
12. Ibid., 5.
13. Ibid., 53.
14. Bull, 64–68.
15. The debate regarding polarity and its effects is a vibrant one. See Stuart J. Kaufman, Richard Little, and William C. Wohlforth, eds., *The Balance of Power in World History* (New York: Palgrave Macmillan, 2007), for an excellent representation regarding the state of debate.
16. While a formalized theory of cyberspace and its relation to international politics has yet to be devised, there are several excellent attempts indicating movement in this direction. See Panayotis A. Yannakogeorgos, "Internet Governance and National Security," *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 102–25; and Katharina Ziolkowski, ed., *Peacetime Regime for State Activities in Cyberspace* (Tallin: NATO, 2013). See also Yannakogeorgos "Cyberspace, The New Frontier—and the Same Old Multilateralism," in *Global Norms, American Sponsorship and the Emerging Patterns of World Politics*, ed. Simon Reich (Hampshire, UK: Palgrave Macmillan, 2010).
17. Daniel T. Kuehl, "From Cyber-space to Cyber-power: Defining the Problem," in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington: Potomac Books, 2009), 28.
18. Waltz, *Theory of International Politics*, 143.
19. David J. Betz and Tim Stevens, *Cyberspace and the State* (London: International Institute for Strategic Studies, 2011), 12.
20. Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), 30–31.

21. David J. Lonsdale, *The Nature of War in the Information Age* (London: Frank Cass, 2004), 135.
22. Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 234.
23. Karl Popper, ed., *The Poverty of Historicism* (New York: Routledge, 2010), 148.
24. Quincy Wright, *A Study of War: Second Edition with a Commentary on War since 1942* (Chicago: University of Chicago Press, 1965).
25. See Mancur Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups* (Cambridge: Harvard University Press, 1971), 36–43.
26. There should be no expectation that the costs of governing the cyberspace or the commons will be evenly divided. Even in small groups, there is the tendency for exploitation of the great by the small. See Olson, *Logic of Collective Action*, 27–30.
27. Cecilia Kang and Ian Shapira, “Facebook Treads Carefully after Its Vital Role in Egypt’s Anti-Mubarak Protests,” *Washington Post*, 3 February 2011, <http://www.washingtonpost.com/wp-dyn/content/article/2011/02/02/AR2011020206107.html>.
28. “Turkey Blocks YouTube as Audio of High-Level Meeting on Syria Leaks,” *Lede*, 27 March 2014, <http://thelede.blogs.nytimes.com/2014/03/27/turkey-follows-twitter-ban-with-block-on-youtube-as-audio-of-high-level-meeting-on-syria-leaks/>.
29. Max Fisher, “Hacker Group Anonymous Is No Match for North Korea,” *Washington Post*, 27 June 2013, <http://www.washingtonpost.com/blogs/worldviews/wp/2013/06/27/hacker-group-anonymous-is-no-match-for-north-korea/>.
30. Peter Dicken, *Global Shift: Mapping the Changing Contours of the World Economy*, 6th ed. (New York: Guilford Press, 2011), 61.
31. *Ibid.*, 82.
32. Stephen D. Krasner, “Structural Causes and Regime Consequences: Regimes as Intervening Variables,” in *International Regimes*, ed. Krasner (Ithaca, NY: Cornell University Press, 1983), 1. Also see other articles in the same work by Ernst Haas, Donald J. Puchala and Raymond F. Hopkins, Oran R. Young, Arthur A. Stein, Robert Keohane, Robert Jervis, John Gerard Ruggie, and Krasner.
33. Robert O. Keohane, *After Hegemony: Cooperation and Discord in the World Political Economy* (Princeton: Princeton University Press, 2005), 88–95.
34. Emanuel Adler, “The Emergence of Cooperation: National Epistemic Communities and the International Evolution of the Idea of Arms Control,” in *Knowledge, Power, and International Policy Coordination*, ed. Peter Haas (Columbia: University of South Carolina Press, 1997), 101.
35. *Ibid.*, 102.
36. *Ibid.*, 145.
37. Brent Williams, “Ten Propositions Regarding Cyberspace Operations,” *Joint Force Quarterly* 61 (April 2011): 18.
38. Polarity seems to have something to do with regime creation. The activity during the Cold War illustrates this—during this time, regimes emerged and thrived in the areas of arms control, trade, and human rights, to name a few.

39. See Gary Brown and Keira Pollett, "The Customary International Law of Cyberspace," *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 141.

40. "NTIA Announces Intent to Transition Key Internet Domain Name Functions," news release, 14 March 2014, <http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions>.

### **Disclaimer**

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: [strategicstudiesquarterly@us.af.mil](mailto:strategicstudiesquarterly@us.af.mil).